Information Security Managers Group
Thursday, August 26, 2010 Meeting Minutes

MEETING LOGISTICS (all meeting minutes are posted on the ISMG Sharepoint site: http://ent.sharepoint.mt.gov/groups/ism/default.aspx)

When: Last Thursday of each month 1:00 pm – 2:30 pm
Who: Agency CIO and/or Information Security Manager
Where: Department of Labor and Industry First Floor Conference Room
Corner of Lockey and Sanders
Next Meeting: Tentative – September 30, 2010 1:00 pm

PRESENT

MDT:	Kristi Antosh
DLI:	Judy Kelly
DOA:	Kevin Winegardner – Chair
DOA:	Larry Manchester
OPI:	Jim Gietzen
HHS:	Jacklynn Thiel
DOR:	Cleo Anderson
DEQ:	Michael Jares
FWP:	Barney Benkelman
DNR:	Rick Bush

PURPOSE

The Information Security Managers Group has three primary purposes:

- Advise the State CIO on Information Risk Management Issues at the Statewide level
- Raise awareness while identifying communities of interest for EPP purposes
- Provide a forum for agency exchange of information

AGENDA ITEMS

- **Welcome and (re)introductions**
  - It was identified that the players already knew each other and introductions were not necessary.

- **Training on NIST Controls – Control Family – Program Management Control PM-3 "Information Security Resources"**
  - Discussion:
    - Postponed until Sept. 2010 meeting.

- **Discussion– Objective's in the sample Information Security Program plan**
  - Chair to post to ISMG Sharepoint site for membership review prior to next ISMG meeting in Sept. 2010

- **Status Update: State CIO decision package legacy IT policies:** Logging On and Logging Off Computer Resources and Remote Access for Employees and Contractors
  - State CIO is reviewing decision package recommending revising legacy IT security policies into a "Statewide Standard: Access Control", and "Statewide Guideline: Access Control", suspense date is 20100915.

- **Action Item: Discuss and provide recommendation to Chair for State CIO decision package on legacy IT policies:** Internet and Intranet Security and Internet Filtering.
    - Review: The team applied previously determined criteria for a Statewide Information Security Policy, to the legacy IT policies under discussion to determine if they meet the criteria:
        - Statewide IT Security Policies must comply with State Statutes.
            - Determination: Fail.
                - The Internet Filtering policy is not an IT Security issue.
            - Determination: Pass.
                - The Internet and Intranet Security policy does not exceed State Statute.
        - Statewide IT Security Policies must be broadly applicable to all covered entities.
            - Determination: Fail.
                - The Internet and Intranet Security policy is very narrow in scope applying primarily to DOA/ITSD as the State IT service provider of Internet/Intranet services.
                - The Internet Filtering policy applies primarily to DOA/ITSD as the State IT service provider of the Internet Filter.
        - Statewide IT Security Policies must align and address NIST Control Families at a Strategic level
            - Determination: Fail.
                - The Internet and Intranet Security policy applies at the technical security control level for IT service provider of internet and intranet services. It mainly specifies 'terms of service' and some features of the service, under which the IT service provider will provide its internet and intranet services. Section B: Agency Internet/Intranet Responsibilities is redundant with MCA 2-15-114 and superseded by Statewide Policy: Information Security Programs.
                - The Internet Filtering policy is a Customer Service Procedure to request internet service access changes, (either blocking or allowing access to web sites), to the standard internet service access provided by the IT service provider.
    - Recommendation of Development Team:
        - Of the three courses of action the development team was tasked to select from in reviewing the legacy IT policies:
            - Retain as written
            - Revise to align with NIST
            - Rescind the legacy IT policy
        - Based on the determination that the Policies fail to meet all minimum criteria to qualify as a Statewide IT Security Policies the team decided to recommend:
            - Rescind the legacy IT Internet and Intranet Security policy.
                - The team notes that the IT service provider has created and is following NIST policies and procedures at the operational and technical level that address this issue; additionally the team is aware that the IT service provider is addressing the larger 'terms of service' issue as well.
            - Rescind the legacy IT Internet Filtering policy.

- The team notes that this is a Customer Service Procedure to request changes in the IT service provider's internet service access, and that the IT service provider has already determined a standard configuration of internet service access.
- The team does recommend that the standard configuration of the internet service access being provided by the IT service provider be specified in the providers service catalog (i.e.; what web sites/categories are blocked).
- The team also requested that this be raised to Enterprise HR as an issue since several agencies point to this current policy for their individual HR user appropriate access enforcement activities.

- **ISMG** postponed the review and discussion of possible training opportunity by having MISTI bringing, 'Applying the NIST Information Risk Management Framework' and 'Managing an Information Security Program' seminars to the state. See complete list of seminars here: http://www.misti.com/default.asp?Page=31&Type=3&Cat=168
  - Postponed until Sept. meeting

ACTION ITEMS

- Review sample "Statewide Standard: IS Identification and Authentication" posted on the ISMG Sharepoint site http://ent.sharepoint.mt.gov/groups/ism/irmp/Policy%20Instruments/Forms/AllItems.aspx
  - Development Team

- Refine the Objective's in the sample Information Security Program plan and post for discussion on the ISMG site.
  - ISMG Chair

- Craft and post a draft decision package on the ISMG Sharepoint site for ISMG review at the Sept. meeting containing the above recommendations regarding the legacy IT security policies Internet and Intranet Security and Internet Filtering.
  - ISMG Chair

- Develop a visual representation of Policy, Standard of Performance, Guideline, and Procedure taxonomy. Post to ISMG Sharepoint site. (Companion Visual to go with spreadsheet "Connect Dots Ext Req to Procedures" here: http://ent.sharepoint.mt.gov/groups/ism/ate/Policy%20Standard%20Guidelines%20Procedures%20Taxonomy/Forms/AllItems.aspx
  - ISMG Chair

- Develop a visual representation of Sample Program Implementation Strategy. Post to ISMG Sharepoint site. (Companion Visual to go with "Sample Program Implementation Strategy" document here: http://ent.sharepoint.mt.gov/groups/ism/irmp/Planning/Forms/AllItems.aspx?RootFolder=%2fgrou

ps%2fism%2firmp%2fPlanning%2fNear%2dTerm&FolderCTID=&View=%7b9FBC1CC6%2dA447%2d4B8F%2d8F78%2d2B1E6E645E87%7d)

- ISMG Chair

AGENDA ITEMS FOR NEXT MEETING

- Training on NIST Controls – Control Family – Program Management Control PM-3– "Information Security Resources" Integrating the Information Security Program resource requirements into the Capital Planning and Investment Control process
  - ISMG Chair

- Review and discuss refined Objective's in the sample Information Security Program plan
  - ISMG

- Report on Status: Decision Package for the State CIO, recommending revising legacy IT security policies Logging On and Logging Off Computer Resources and Remote Access for Employees and Contractors into a "Statewide Standard: Access Control", and "Statewide Guideline: Access Control"
  - ISMG Chair

- Review and discuss: sample "Statewide Standard: IS Identification and Authentication" for requirements determination
  - Development Team (ISMG)

- Approve decision package for State CIO regarding the legacy IT security policies Internet and Intranet Security and Internet Filtering
  - Development Team (ISMG)

- Discuss and Determine recommendation on next legacy IT policies under review*: To be determined
  - Development Team (ISMG)